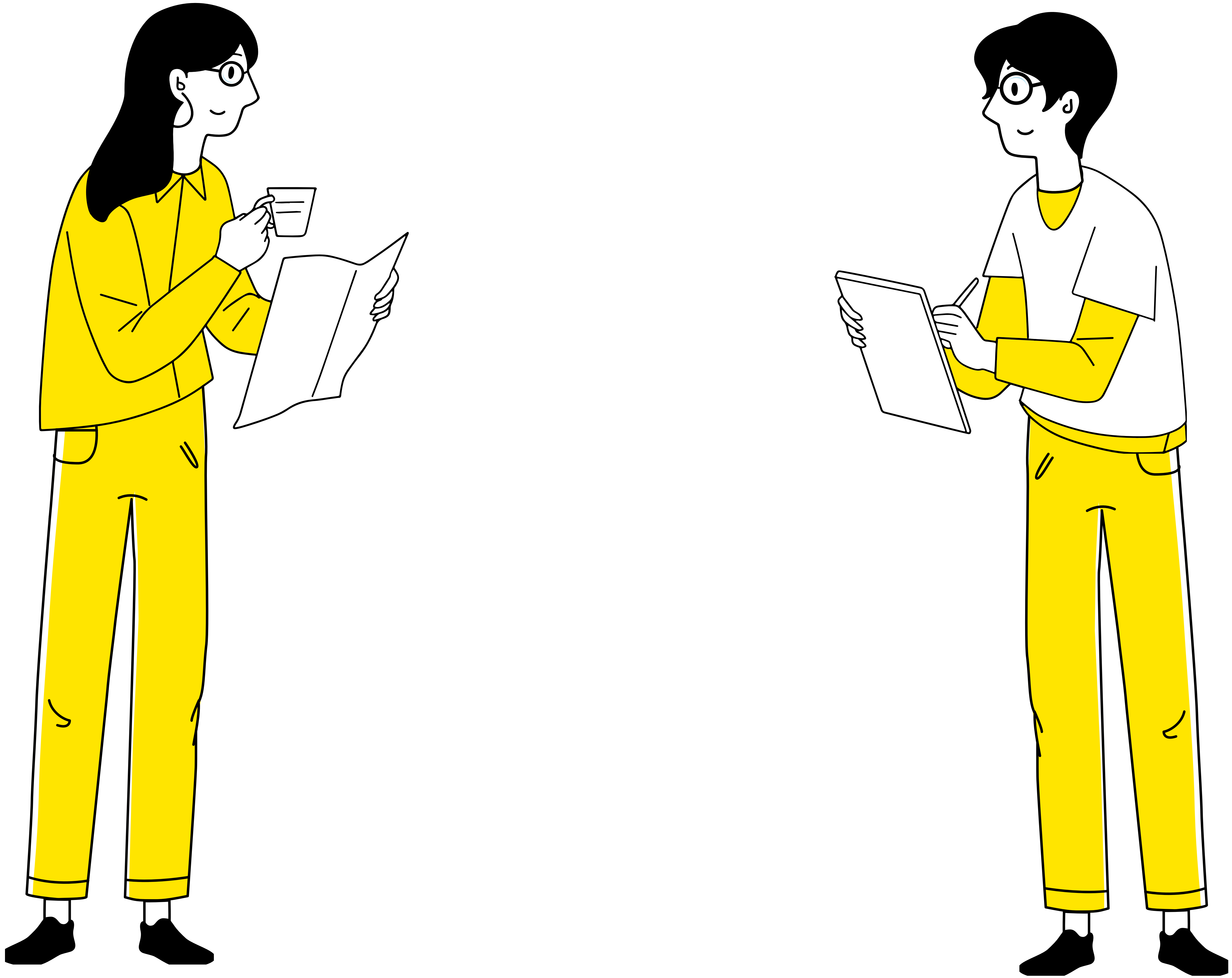
LIP6 ALMASTY Seminar
February 17th, 2022.

Paola de Perthuis

MyOPE

Malicious securitY for Oblivious Polynomial Evaluation

Joint work of:
Malika Izabachène - Cosmian
Anca Nitulescu - Protocol Labs
David Pointcheval - ENS Paris
Paola de Perthuis - ENS/Cosmian



Alice
Receiver/Verifier

Secret Evaluation Point

m

Bob
Sender/Prover

Secret Polynomial

$$\mathsf{f}(Y) = \sum_{j=0}^{N} \mathsf{f}_j Y^j$$

Alice

Receiver/Verifier

Secret Evaluation Point

m

Bob

Sender/Prover

Secret Polynomial

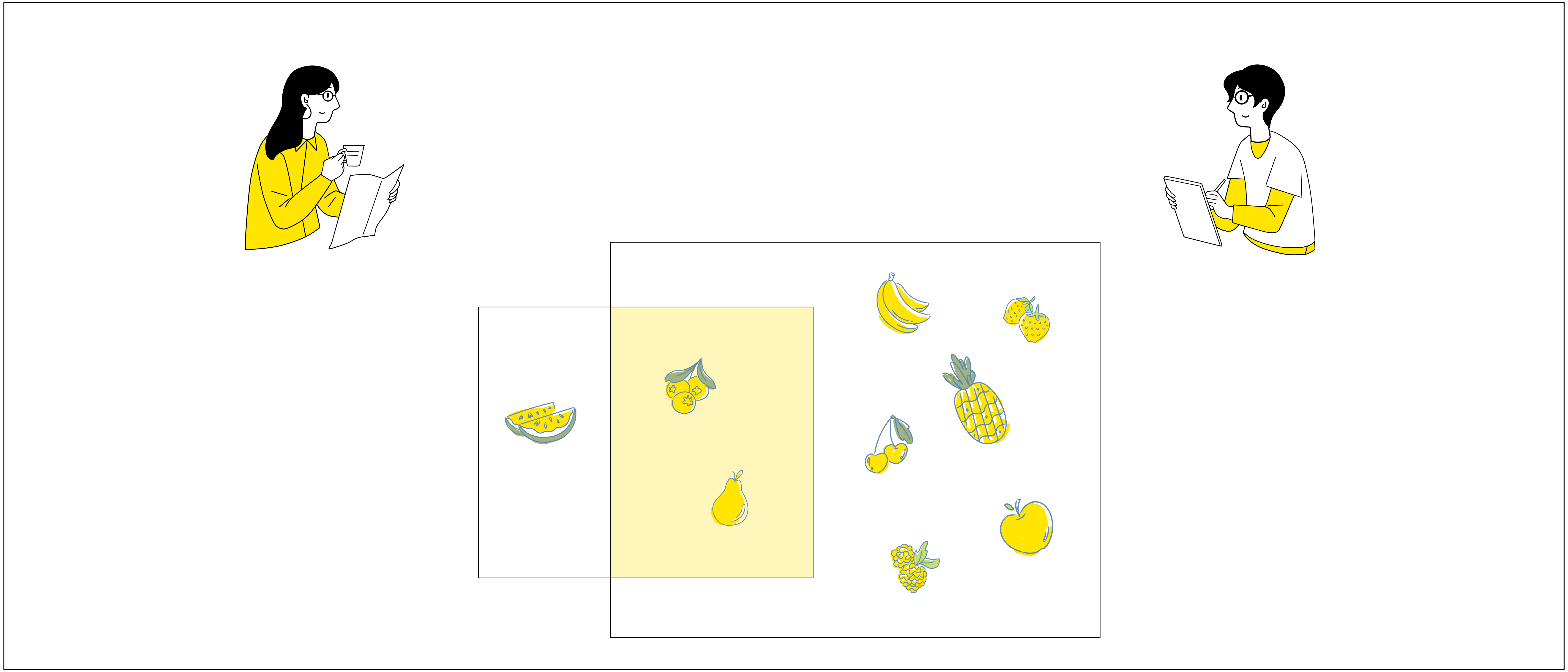
$$\mathsf{f}(Y) = \sum_{j=0}^{N} \mathsf{f}_j Y^j$$

Alice wants to get the evaluation of Bob's polynomial in her point:

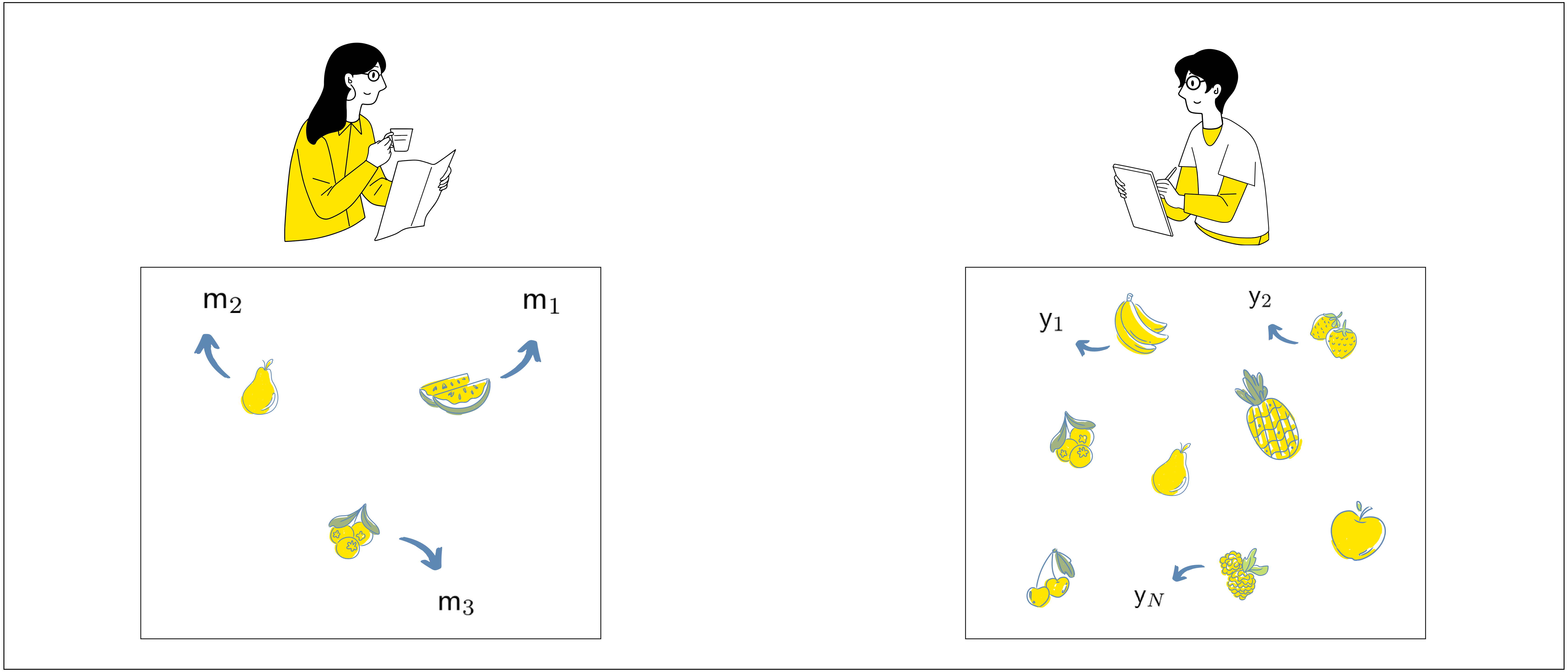
$$\sum_{j=0}^{N} \mathsf{f}_j \mathsf{m}^j$$

Use case: Private Set Intersection (PSI)

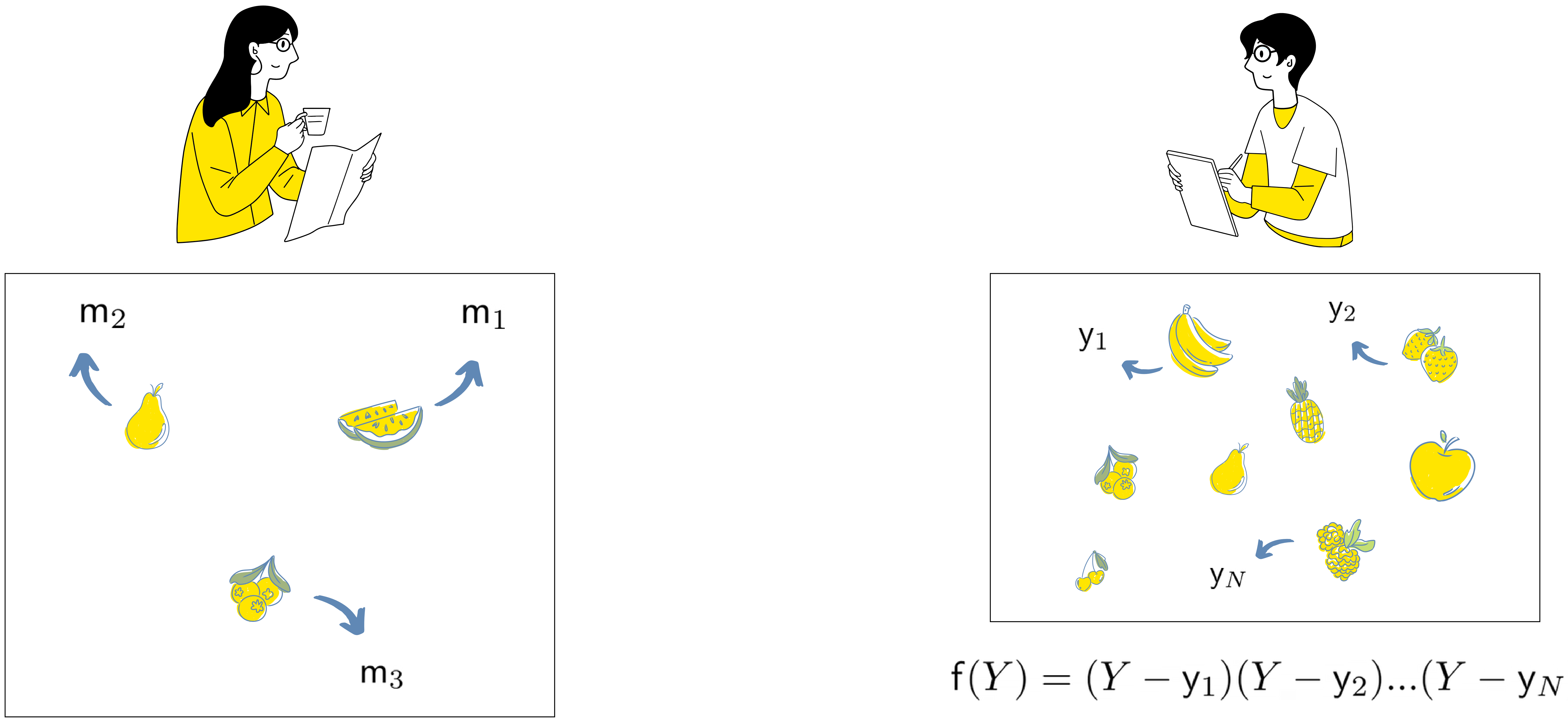
Use-case: PSI



PSI

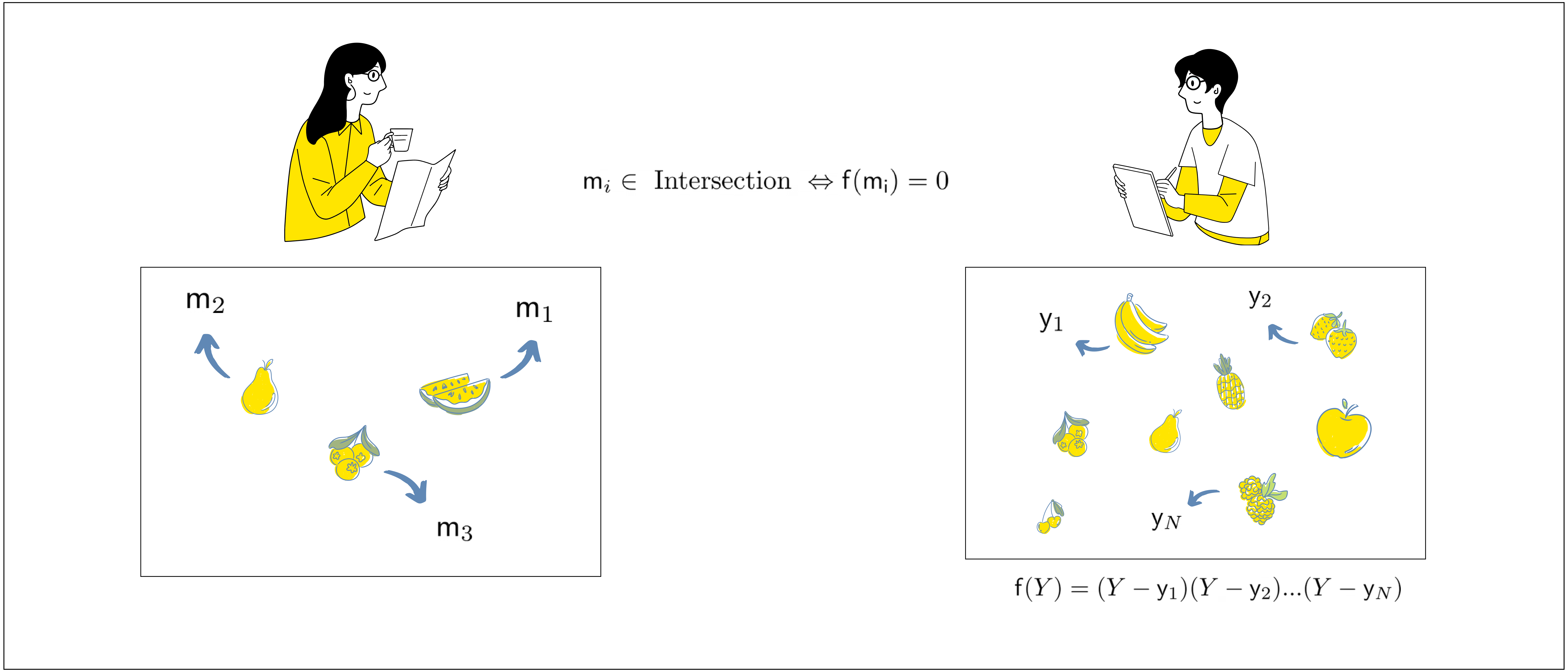


PSI



$$f(Y) = (Y - y_1)(Y - y_2)\ldots(Y - y_N)$$

Example of PSI



Motivation.
In the litterature we found...

1. ...No active security [CLR17]
2. ...Security only against a malicious receiver [CHLR18]
3. ...Security against a malicious sender but for non-FHE methods incurring higher asymptotic communication complexity and recurring setup phases [HL09, GNN17, Haz18]
4. We give a construction for compact verification of inner-product computations.
5. Our method can be extended to SPIR
6. We are best adapted to the unbalanced setting with a greater sender set size

In the litterature

2009

Efficient Oblivious Polynomial Evaluation with Simulation-Based Security
Hazay - Lindell

2017

Fast Private Set Intersection from Homomorphic Encryption
Chen - Laine - Rindal

Maliciously Secure Oblivious Linear Function Evaluation with Constant Overhead
Ghosh - Nielsen - Nilges

2018

Labeled PSI from Fully Homomorphic Encryption with Malicious Security
Chen - Huang - Laine - Rindal

Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs
Hazay

2020

Boosting Verifiable Computation on Encrypted Data
Pointcheval - Nitulescu - Fiore

Flexible and Efficient Verifiable Computation on Encrypted Data
Bois - Cascudo - Fiore - Kim

Using FHE to reduce Communications

Alice
Receiver/Verifier

Secret Evaluation Point

$$\mathsf{m} \in \mathcal{R}_t$$

$\mathcal{R}_t = \mathbb{Z}_t[X]/\mathsf{r}(X)$, r irreducible polynomial of degree n

Bob
Sender/Prover

Secret Polynomial

$$\mathsf{f}(Y) = \sum_{j=0}^{N} \mathsf{f}_j Y^j, \mathsf{f_j} \in \mathcal{R}_t$$

Using FHE to reduce Communications

Secret Evaluation Point

$$\mathsf{m} \in \mathcal{R}_t$$

FHE Encryption

$$\mathsf{Enc}(\mathsf{m}) = (\mathsf{c}, \mathsf{c}') \in \mathcal{R}_q^2$$

$$\mathsf{Enc}(\mathsf{m}^i) \times \mathsf{Enc}(\mathsf{m}^j) = \mathsf{Enc}(\mathsf{m}^{i+j})$$

$$\mathsf{Dec}\Big(\sum_{j=0}^{N} \mathsf{f}_j \cdot \mathsf{Enc}(\mathsf{m}^j)\Big) = \sum_{j=0}^{N} \mathsf{f}_j \mathsf{m}^j$$

Secret Polynomial

$$\mathsf{f}(Y) = \sum_{j=0}^{N} \mathsf{f}_j Y^j, \mathsf{f}_\mathsf{j} \in \mathcal{R}_t$$

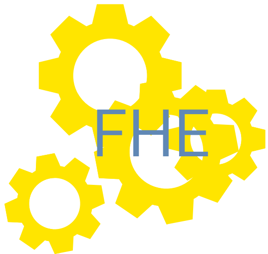
Using FHE to reduce Communications

$\mathsf{m} \in \mathcal{R}_t$

FHE Encryption

$\mathsf{Enc}(\mathsf{m}) = (\mathsf{c}, \mathsf{c}') \in \mathcal{R}_q^2$

+ intermediate powers' ciphertexts



$(\mathsf{u}_i, \mathsf{u}'_i) = \mathsf{Enc}(\mathsf{m}^i), \forall i \in [\![0; N]\!]$

Verifiability

1. We will need to prove the computation of scalar products with respect to commited vectors is correct.

2. Some of these vectors could be private.

Verifiable Inner-Product

for public vectors

Verifiable Inner-Product

$$\mathsf{A} = (a_0, \ldots, a_N), \mathsf{B} = (b_0, \ldots, b_N) \in \mathbb{Z}_q^{N+1}, c = \langle \mathsf{A}; \mathsf{B} \rangle$$

We define:

$$\bar{\mathsf{a}}(Y) = \sum_j a_j Y^{N-j}, \qquad \mathsf{b}(Y) = \sum_j b_j Y^j \in \mathbb{Z}_q[Y^N]$$

The N-degree coefficient of the product of these polynomials is c. The polynomial:

$$\mathsf{d}(Y) = \bar{\mathsf{a}}(Y) \cdot \mathsf{b}(Y) - cY^N \in \mathbb{Z}_q[Y^{2N \setminus N}]$$

has no term of degree N.

The prover commits a, b, and d into the appropriate subspaces of the space of polynomials with coefficients mod q.

Committing a polynomial

1. Linear-Only Encodings
2. Compactness sending evaluations in random points
3. The encoding scheme allows the verification of quadratic relations from the commitments.

Commitment

Twin encodings of the polynomial evaluations in K random secret points, K=1 if q is prime, the second encoding with a secret random scalar specific to the subspace.
The scalars are known to the verifier and the prover commits with linear combinations of public encodings of the point monomials.

$$\mathsf{E}(\mathsf{u}(s_k)) = \sum_j u_j \mathsf{E}(s_k^j) \qquad \mathsf{E}(r \cdot \mathsf{u}(s_k)) = \sum_j u_j \mathsf{E}(r s_k^j)$$

Proof

The prover provides evaluations of the polynomial in M random points, M=1 if q is prime, and proves they are consistent with the commitments of the polynomial using v_m defined with:

$$\mathsf{u}(Y) - \mathsf{u}(y_m) = (Y - y_m) \cdot \mathsf{v}_m(Y)$$

providing encodings of evaluations of the v_m in all the K secret points.

Schwartz-Zippel Lemma

if q is a prime, $\mathsf{p} \in \mathbb{Z}_q[Y^N]$ a non-zero polynomial of degree at most N,

then for a random $s \in \mathbb{Z}_q$, and $e \in \mathbb{Z}_q$, the probability that $\mathsf{p}(s) = e$ is bounded by:

$$\mathbb{P}(\mathsf{p}(s) = e) \leq \frac{N}{q}$$

More generally, if q is a product of ℓ primes factors greater than $p \in \mathbb{Z}$, then:

$$\mathbb{P}(\mathsf{p}(s) = e) \leq \frac{N\ell}{p}$$

Hence the probability for two different polynomials to have the same evaluation in a random point.

This gives the necessary number of repetitions, which become more than 1 in the RNS compatible setting

Committing a polynomial

1. Linear-Only Encodings
2. Compactness sending evaluations in random points
3. The encoding scheme allows the verification of quadratic relations from the commitments.

Commitment

Twin encodings of the polynomial evaluations in K random secret points, K=1 if q is prime, the second encoding with a secret random scalar specific to the subspace.
The scalars are known to the verifier and the prover commits with linear combinations of public encodings of the point monomials.

$$\mathsf{E}(\mathsf{u}(s_k)) = \sum_j u_j \mathsf{E}(s_k^j) \qquad \mathsf{E}(r \cdot \mathsf{u}(s_k)) = \sum_j u_j \mathsf{E}(r s_k^j)$$

Proof

The prover provides evaluations of the polynomial in M random points, M=1 if q is prime, and proves they are consistent with the commitments of the polynomial using v_m defined with:

$$\mathsf{u}(Y) - \mathsf{u}(y_m) = (Y - y_m) \cdot \mathsf{v}_m(Y)$$

providing encodings of evaluations of the v_m in all the K secret points.

Verifiable Inner-Product

$$\mathsf{A} = (a_0, \ldots, a_N), \mathsf{B} = (b_0, \ldots, b_N) \in \mathbb{Z}_q^{N+1}, c = \langle \mathsf{A}; \mathsf{B} \rangle$$

We define:

$$\bar{\mathsf{a}}(Y) = \sum_j a_j Y^{N-j}, \qquad \mathsf{b}(Y) = \sum_j b_j Y^j \in \mathbb{Z}_q[Y^N]$$

The N-degree coefficient of the product of these polynomials is c. The polynomial:

$$\mathsf{d}(Y) = \bar{\mathsf{a}}(Y) \cdot \mathsf{b}(Y) - cY^N \in \mathbb{Z}_q[Y^{2N \setminus N}]$$

has no term of degree N.
The prover commits a, b, and d into the appropriate subspaces of the space of polynomials with coefficients mod q.

The relation between a, b, d, and c is proven using a quadratic check.

Verifiable Inner-Product

with a private vector
we use hiding
commitments

In our protocol we grant privacy with FHE ciphertexts

We need to perform scalar products with vectors whose coefficients are polynomials.

Verifiable Inner-Product

between vectors whose
terms are polynomials

Verifiable Inner-Product

between vectors whose terms are polynomials

We use commitments of bivariate polynomials

Verifiable Inner-Product

between vectors whose terms are polynomials

We use commitments of bivariate polynomials

We also commit the vectors where the terms are evaluated in a random point

Verifiable Inner-Product

between vectors whose terms are polynomials

We use commitments of bivariate polynomials

We also commit the vectors where the terms are evaluated in a random point

We prove consistency between them with quadratic checks

Verifiable Inner-Product

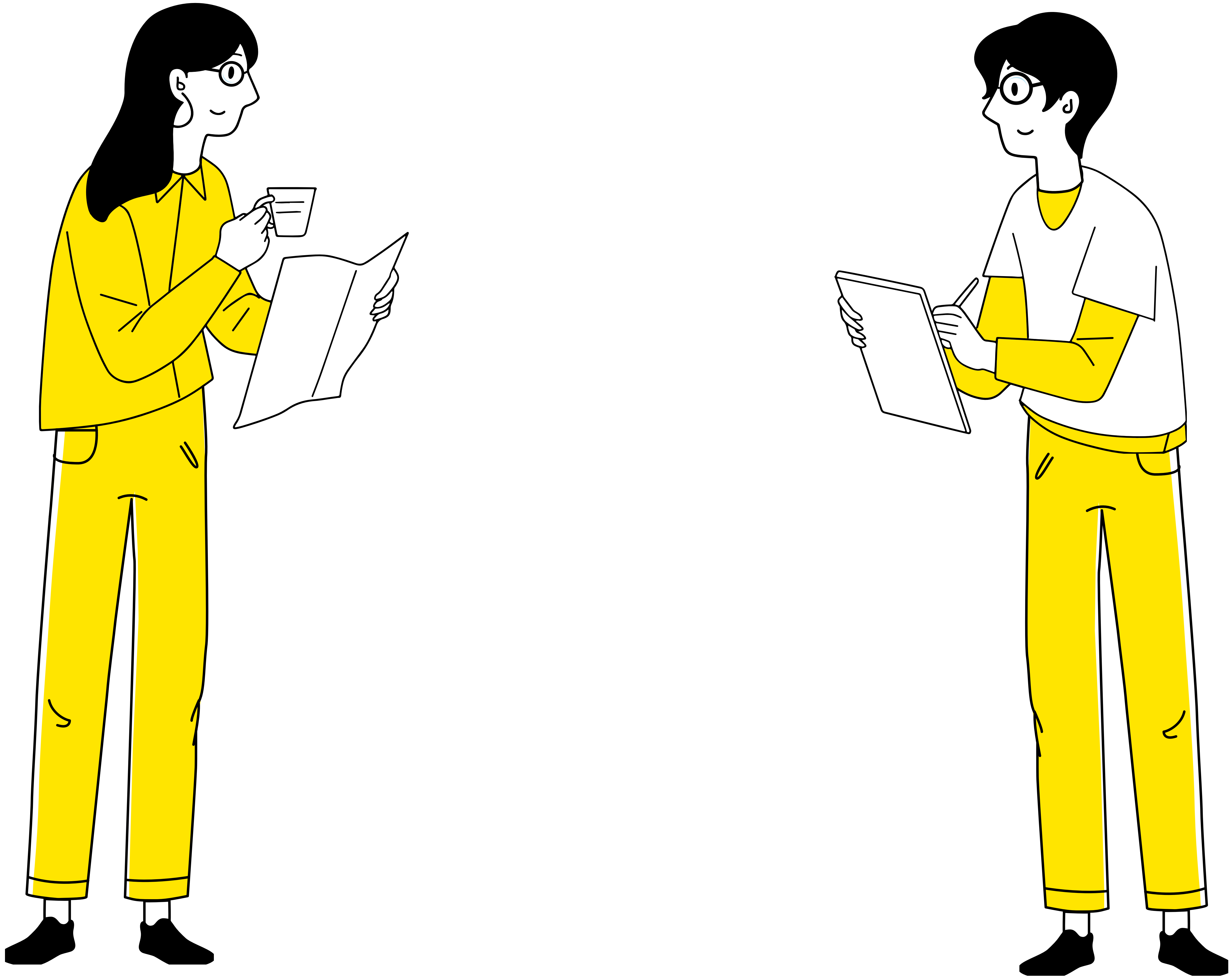
between vectors whose terms are polynomials

We use commitments of bivariate polynomials

We also commit the vectors where the terms are evaluated in a random point

We prove consistency between them with quadratic checks

We prove the inner-product relation on the univariate polynomials



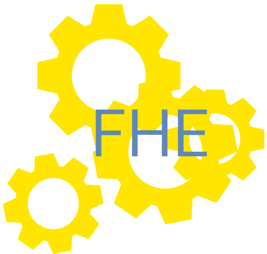
Back to Oblivious Polynomial Evaluation

$\mathsf{m} \in \mathcal{R}_t$

FHE Encryption

$\mathsf{Enc}(\mathsf{m}) = (\mathsf{c}, \mathsf{c}') \in \mathcal{R}_q^2$

+ intermediate powers' ciphertexts



$(\mathsf{u}_i, \mathsf{u}'_i) = \mathsf{Enc}(\mathsf{m}^i), \forall i \in [\![0; N]\!]$

Are the (uj,uj')'s correct?

Alice picks a random element n, and asks for:

$$\langle(\mathsf{n}^0,\ldots,\mathsf{n}^N);(\mathsf{u}_0,\ldots,\mathsf{u}_N)\rangle$$

$$\langle(\mathsf{n}^0,\ldots,\mathsf{n}^N);(\mathsf{u}'_0,\ldots,\mathsf{u}'_N)\rangle$$

She checks the following decryption once the inner products are proven:

$$\mathsf{Dec}(\sum_j \mathsf{n}^j(\mathsf{u}_j,\mathsf{u}'_j)) = \sum_j \mathsf{n}^j\mathsf{m}^j$$

Are the (uj,uj')'s correct?

Alice picks a random element n, and asks for:

$$\langle (\mathsf{n}^0, \ldots, \mathsf{n}^N); (\mathsf{u}_0, \ldots, \mathsf{u}_N) \rangle$$

$$\langle (\mathsf{n}^0, \ldots, \mathsf{n}^N); (\mathsf{u}'_0, \ldots, \mathsf{u}'_N) \rangle$$

She checks the following decryption once the inner products are proven:

$$\mathsf{Dec}(\sum_j \mathsf{n}^j (\mathsf{u}_j, \mathsf{u}'_j)) = \sum_j \mathsf{n}^j \mathsf{m}^j$$

With t $\equiv$ 3 mod 4, $\mathcal{R}_t$ is a product of two large fields, hence the Schwartz-Zippel lemma gives the soundness.

Then the OPE inner-product is proven

The polynomial evaluation ciphertext is given by the inner-products of the (uj)j, (u'j)j vectors with the vector of coefficients of f.

She will see the noise in the ciphertexts when she decrypts

What if Alice learnt from Bob's noise?

That noise carries information about Bob's polynomial, f, which was used in the linear combinations of public ciphertexts of powers of m

Noise flooding for security against an honest-but-curious Alice

$$(\tilde{\mathsf{d}} = \sum_j \mathsf{u}_j \cdot \mathsf{f}_j + \mathsf{z}^* - \mathsf{q}^* \cdot \mathsf{r}, \tilde{\mathsf{d}}')$$

$$\mathsf{Dec}(\tilde{\mathsf{d}}, \tilde{\mathsf{d}}') = \sum_{j=0}^{N} \mathsf{f}_j \mathsf{m}^j$$

Noise flooding

to protect Bob's privacy against an honest-but-curious Alice.

$$(\tilde{\mathsf{d}} = \sum_j \mathsf{u}_j \cdot \mathsf{f}_j + \mathsf{z}^* - \mathsf{q}^* \cdot \mathsf{r}, \tilde{\mathsf{d}}')$$

Additional noise

$$\mathsf{Dec}(\tilde{\mathsf{d}}, \tilde{\mathsf{d}}') = \sum_{j=0}^{N} \mathsf{f}_j \mathsf{m}^j$$

How can we be sure Bob adds noise and not something else?

We should prove the norm of the added noise polynomials is small.

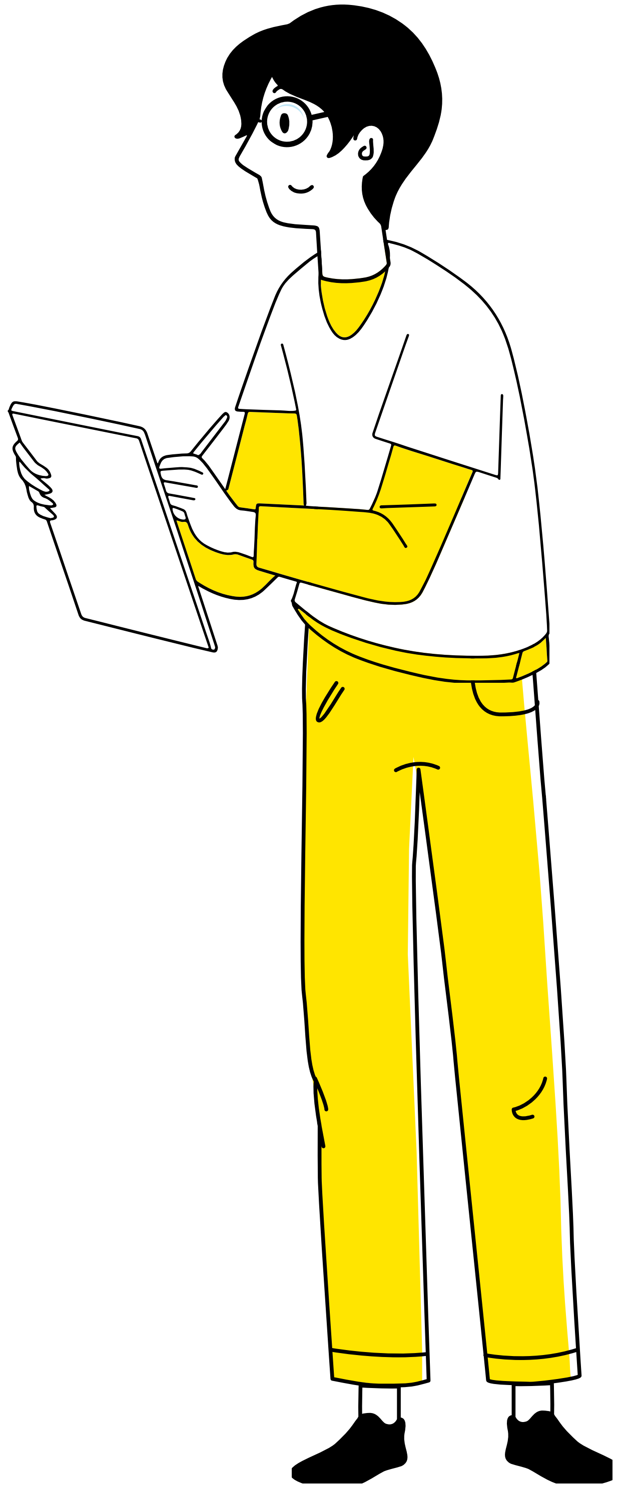
How can we be
... b adds
... nd not
... hing
... ?

That is just another inner-product proof, with a secret committed result and a range proof to make sure it is small enough

We should prove the norm of the added noise polynomials is small.

If a malicious Alice sent incorrect intermediate ciphertexts?

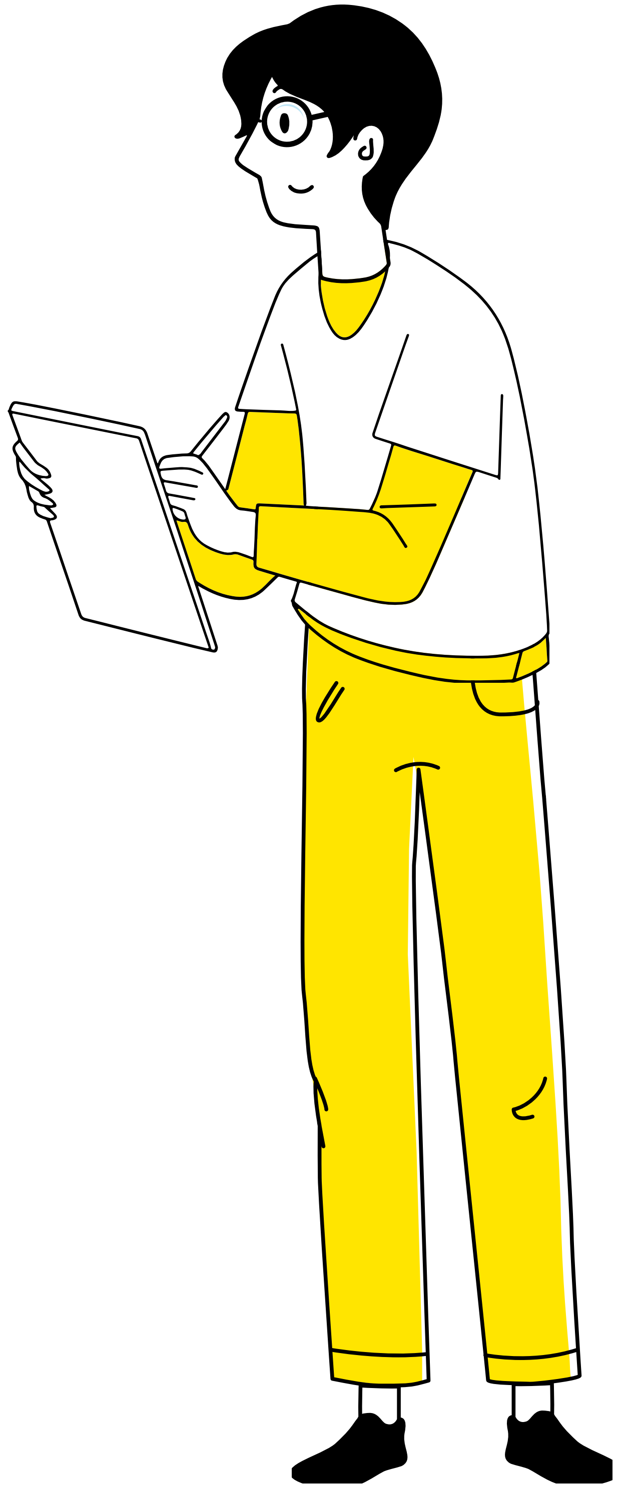
We provide an informal construction, its formal proof would have a high cost



If a m… sent
incor… iate

relationships between powers of the message enables the calculation of a ciphertext which is supposedly of zero with quadratic operations between the intermediate ciphertexts.
Alice can prove it is a ciphertext of zero.

We provide an informal construction, its formal proof would have a high cost



Conclusion

1. Sub-linear communications in $\tilde{O}(N^{2/d})$

2. Security against malicious Bob (+informal construction against a malicious Alice)

3. We provide guidelines to use MyOPE with RNS optimisations for FHE and the SEAL library

4. Small proof sizes in $\tilde{O}(1)$

5. Compact proofs of inner-products are of independent interest

6. Extension to Symmetric Private Information Retrieval

7. Straightforward adaptation to dynamic databases

8. N on 30 bits, n on 14 bits, q on less than 512 bits, t=3 => FHE ciphertexts are less than 200MB, the proof on less than 100KB, for 128 bits of security.

MyOPE @ALMASTY Seminar
Feb. 17th, 22.

Paola de Perthuis

Thank you!